Common Criteria

Using the Common Criteria (CC) in Smart Card Security

Panel Chair:

Stuart Katzke, Chief Scientist, Information Assurance Solutions Group, NSA

Panelists:

Gilles Lisimaque, Chief Technology Officer, Gemplus Corp.

Kenneth Ayer, Director, Chip Card Security, Visa International

Gene Troy, Chair Smart Card Security User Group, NIST

Presentations

- ***Introduction to Smart Card Technology,*** **Gilles Lisimaque, Chief Technology Officer, Gemplus Corp.**
- ***User's Perspective on Smart Card Security*****, Kenneth Ayre, Director, Chip Card Security, Visa International**
- ***NIAP and CC-based (ISO 15408) Evaluation,*** **Gene Troy, Chair Smart Card User Group, NIST**

Key Messages

- Smart card developers, the financial industry smart card issuers, and the government are working cooperatively in the Smart Card Users Group (SCSUG) to improve the security of smart cards and their use in financial applications through:
  1) development and adoption of security requirements for the physical, operating system, and application aspects of smart cards
  2) assurance that smart card security requirements are being met and that vulnerabilities have been eliminated or reduced

Key Messages (cont.)

- The NIAP CC-based validation scheme provides a neutral, independent evaluation capability that all participants in the Smart Card Users Group trust.
- The SCSUG participants believe that CC-based evaluations of smart card security requirements will result in the comparability of test results performed by NIAP and other international CC-based labs.

Issues Addressed

- **Variety of Security Challenges to Smart Cards:**
  - **small but complex & highly trusted object**
  - **control or represent valuable assets**
  - **held & used by untrusted users**
- **Secure Development, Functioning, & Testing**
- **Use of the Common Criteria/ISO 15408-based Process for Defining Security Requirements & Using the Requirements in Product Evaluations**